Electronic Version

Stylesheet Version v1.1.1

Description

A method for dense and secure transmission of signals and information using a small number of channels

Cross Reference To Related Applications

[0001] This application claims priority from U.S. provisional patent application Ser. No. 60/500,145 filed September 1, 2003.

Background of Invention

[0002] The extreme bandwidth of a single optical fiber (25 000 GHz) is 1000 times larger than the total radio bandwidth of planet Earth (25 Ghz). Using this bandwidth effectively requires novel network designs.

[0003] Suppose that there are given n Senders $S_1,S_2,...,S_n$ and r Receivers $R_1,R_2,...,R_r$. Let p be a function from {1,2,...,n} to {1,2,....,r}. Our goal is to send long messages from S_i to $R_{p(i)}$, for i=1,2,...,n such that

[0004] $R_{p(i)}$ can easily retrieve the message of S_i, for i=1,2,...,n,

and

[0005] $R_{p(i)}$ cannot retrieve the message of S_j if p(i) is not equal to p(j).

[0006] An obvious method for doing this is connecting S_i with $R_{p(i)}$ with private channels, that is, we use n channels for the n Senders and the r Receivers. The advantage of this solution is that n bits can be sent in parallel, and the transmission is private, in the sense that $R_{p(i)}$ receives only the transmission of S_i, for i=1,2,...,n. The privacy is satisfied only if others have not access to the private channels. The disadvantage of this solution is that the number of channels is equal to the number of communicating pairs, and this is infeasible in most cases.

[0007] Another problem with this solution is that if next time S_i wants to send messages to $R_{s(i)}$, for i=1,2,....,n for some other function s, then the whole network has to be reconfigured. If every Sender is directly connected to all Receivers, this solves the reconfiguration problem, but then the number of channels becomes nr. Applying some classical interconnection networks (e.g., the butterfly, Benes network, CCC) needs routers with buffers (local memory). Due to the table-lookup features of routers and the need of optical memory, all-optical routers are hard to con-

struct, expensive and still relatively slow components.

[0008] Another obvious solution is that all the Senders and Receivers use the same channel, and they transmit their messages one after the other. Transmitting n bits this way needs n steps. In this case either a router has to be used just before the messages get to the Receivers, or some sort of encryption is needed for maintaining the privacy of the transmission.

[0009] Using encryption has several drawbacks. Streamciphers, the most evident cryptographic tool which are fast and do not cause overhead in the communication have lots of recently proposed and successful attacks. Block-ciphers are much slower, and may be infeasible in, say, in the 1000 Gbit/s range, and also, they causes non-negligible overhead in the communication.

[0010] Using routers and addressing in the messages will also slow down the communication, especially in all-optical environments: with, say, 1000 Gbit/s throughput, by the best of our knowledge, no routers exist.

[0011] References:

[0012] Y.Azar, E.Cohen, A.Fiat, H.Kaplan, and H.Racke: Optimal oblivious routing in polynomial time. In Proceedings of the thirty-fifth ACM symposium on Theory of computing,

pages 383--388. ACM Press, 2003.

[0013] S. Chatterjee and S. Pawlowski: All optical networks, Communications of the ACM, 42(6):74--83, 1999

[0014] C. Dovrolis, D. Stiliadis, and P. Ramanathan: Proportional differentiated services: Delay differentiation and packet scheduling. In SIGCOMM, pages 109--120, 1999

[0015] V. Grolmusz: Computing elementary symmetric polynomials with a sub-polynomial number of multiplications. SIAM Journal on Computing, 32(6):1475--1487, 2003

[0016] K. Hall and K. A. Rauschenbach: All-optical bit pattern generation and matching. Electron. Lett. 32:1214, 1996

[0017] P. Hawkes and G. Rose. Rewriting variables: the complexity of fast algebraic attacks on stream ciphers. Technical report, eprint.iacr.org/2004/081/, 2004

[0018] M. Jinno and T. Matsumoto: Nonlinear Sagnac interferometer switch and its applications, IEEE J. Quantum Electron., 28:875, 1992

[0019] S.A. Plotkin. Competitive routing of virtual circuits in ATM networks.{\em IEEE Journal of Selected Areas in Communications, 13(6):1128--1136, 1995

[0020] A. Poustie, R. J. Manning, A. E. Kelly, and K. J. Blow: All-optical binary counter. Optics Express, 6:69--74, 2000

Summary of Invention

[0021] In the present disclosure we give a description of a network, together with the associated network-protocol, in which

[0022] The n Senders and the r Receivers are connected with only $r^{o(1)}$ channels (Here o(1) denotes a quantity which goes to 0 as r goes to the infinity.) Note, that in practice at most 32 channels are enough. The parallel channels will not speed up the transmission relative to the 1-channel network: the goal of using them is to facilitate the privacy of the communication and the distribution of the messages between the recipients, without any encryption or routers.

[0023] The encoding and decoding is nothing else just linear combinations of the message-bits, and this linear combinations can be computed really fast.

[0024] There are no switching or routing-elements in the network with hard-to implement buffers and local memory, just linear combinations are computed, with fixed connections (channels or wires); moreover, the network components used are simple enough to implement in fast all-optical networks.

[0025] $R_{p(i)}$ can learn only very little about any bit of the message of S_j for any p(j) not equal to p(i), and only a negligible amount of information on longer messages of S_j.

[0026] The security of our network is information-theoretical rather than cryptographical, in the sense that it does not depend on unproven cryptographical primitives.

[0027] In packet-switched networks, the Receivers should know their own identity (say, an IP or MAC address) in order to pick up only those packets from the transmission channels, which are addressed to them. In the disclosed network architecture, the Receivers need not know even their own identity: the bits, intended to be sent to them, will find them securely and automatically.

Brief Description of Drawings

[0028] FIG. 1 is a schematic drawing of our network in the case when the number of the Senders and the Recievers are also n.

[0029] FIG. 2 is a drawing of a preferred embodiment of the invention as a multicasting network.

Detailed Description

[0030] Let S_1, S_2,...,S_n denote the Senders, and let R_1,R_2,...,R_r denote the Receivers.

[0031] Additionally, we have $t<n$ data transmission channels, used for long-distance connection between Senders and Receivers. Each Sender is connected through some modu-

lar addition gates to all of these t channels, while the Receivers may be connected through modular addition gates only to certain subsets of the channels.

[0032] On one channel one bit may be transmitted at a time. If one Sender sends several bits simultaneously to an h element subset of the t long-distance channels, then these bits will travel synchronously on these h channels: that means, that for any i, Receiver R_i will get those bits which were sent simultaneously, from all the long-distance channels, connected to R_i, at the same time. However, we do not suppose that different Receivers get these bits at the same time (it is allowed that farther situated Receivers get the bits later than the closer ones).

[0033] Figure 1 describes the general scheme in the case when n=r. We need that the Sender's bits travel synchronously on the t long-distance channels (item 2). (Note, that this requirement can be assured by using the same wavelength optical signals on each channel, and by compensating for the distance-differences at the Senders side by installing fiber loops: this way the signals - if sent simultaneously by all the senders - will travel synchronously). However, we need not assume that the signals reach all the Receivers at the same time: the Receivers are allowed

to be scattered along the long-distance channels (see Figure 2).

[0034] A general method was shown in (Vince Grolmusz: Low Rank Co-Diagonal Matrices and Ramsey Graphs, Electronic Journal of Combinatorics, Vol. 7, (2000), No. 1, R15) for the construction of n x n matrices A' with 0's in the diagonal and non-zeroes elsewhere modulo a non-prime power integer, denoted by m. Said construction has the main property that said matrices have small rank modulo m, that is, matrix A' can be written as the matrix product B'C' modulo m, where B'is an n x (t-1) and C' is a (t-1) x n matrix with integer elements, where t is a small number relative to n, that is, $t=n^{o(1)}$, where o(1) denotes a positive quantity which goes to 0 as n goes to the infinity.

[0035] It is also known from the prior art, that said matrix A' can be constructed that way, that if m has distinct prime divisors p_1, p_2,...,p_r, then the non-zero elements of matrix A' are either 0 or 1 modulo p_i, for i=1,2,...,r. For example, if m=6, then the non-zero elements of matrix A' are either 3 or 4, modulo 6.

[0036] Let J denote the n x n all-1 matrix. Let us consider the matrix A=J-A'. It contains 1's in the diagonal, and numbers, congruent to zero modulo at least one prime divisor

of m. Returning to the previous example, with m=6, we have that A has either 3 or 4 or 0 outside of the diagonal. Matrix A can be written as the matrix product BC modulo m, where B is an n x t and C is a t x n matrix with integer elements.

[0037] There are several other ways to construct matrices with similarly useful properties than that of A. Such method is known from the prior art (e.g.,Vince Grolmusz: A Note on Explicit Ramsey Graphs and Modular Sieves, Combinatorics, Probability and Computing Vol. 12, (2003) pp. 565-569). Another way is to construct matrix A is as follows: the entry in row i and column j of matrix A is defined as the Hamming-distance of the binary forms of numbers i and j. By this definition we get matrices B and C such that A=BC, where B is an n x t and C is a t x n matrix with integer elements, and t=O(log n).

[0038] The larger the quantity n is, the smaller the quantity t becomes, relative to n.

[0039] Let $x=(x_1,x_2,...,x_n)$ be a sequence of n variables. We can compute the following $t=n^{o(1)}$ linear forms of the x_i's, denoted by $z=(z_1,z_2,...,z_t)$, such that using another linear transform to this z, we get back a representation of the x. More exactly, Let A=BC. Then let z=xB, and

x'=zC=xBC=xA. This forms the main idea of our network architecture.

[0040] First we describe the network in the case when n=r and Sender S_i wants to send bit x_i to Receiver R_i, for i=1,2,...,n.

[0041] Figure 1 gives a schematic description of the network. From bits $x=(x_1,x_2,...,x_n)$, numbers $z=(z_1,z_2,...,z_t)=xB$ are computed with the modular addition gates (item 1). Numbers $z_1,z_2,...,z_t$ are transmitted on the t long-distance channels (item 2). At the receivers' side (item 3), from these $z_1,z_2,...,z_t$ numbers, modular gates (item 4) compute the n coordinates of x'=xBC=xA.

[0042] Note, that generally x' is not equal to x; for example, if m=6, then matrices B and C can be chosen such that x'= x + 4xU + 3xV=xBC=zC=xA, where U and V are n x n matrices with 0' in the diagonal, satisfying that at any non-diagonal position either U or V is zero modulo 6.

[0043] Consequently, for the retrieval of the original message bits x, some further steps should be taken. We disclose a method, called filtering here.

[0044] We describe the transmission-protocol and the filtering method in rounds. In every round, every sender S_i will transmit securely a bit x_i to the corresponding receiver, R_i,

i=1,2,...,r. In u consecutive rounds, every sender will send u bits, that is, sending u-bit messages needs u rounds of the following protocol.

[0045] A round is performed as follows:

[0046] Step 1 - Encoding (item 1) - From the bits of x the mod m integers $z=(z_1,z_2,...,z_t)$ are computed by linear combinations taken modulo m: $z=xB \bmod m$.

[0047] Step 2 (item 2)- Transmission - The mod m numbers $z_1,z_2,...,z_t$ are sent on t channels to the receivers.

[0048] Step 3 - Decoding - The linear transformation $x'=(x'_1,x'_2...,x'_n,=xBC=xA=zC$ is computed modulo m at the receivers' side, and number x'_i is given to receiver R_i, for i=1,2,...,r. (Note, that because of information-theoretical reasons, generally it is not possible to retrieve bit x_i from integer x'_i).

[0049] Step 4 - Pre-Filtering - A random g permutation on the set {1,2,....,n} is generated at the sender's side. Then for j=1,2,...,n, steps 1, 2 and 3 are repeated for $x^{g(j)}$ instead of x, where $x^{g(j)}$ coincides with x, except on position g(j), whereas $x^{g(j)}$ is 0 if it was 1 in x, or 1 if it was 0 in x. Let x''_i denote the coordinate i of $x^{g(j)}CT$.

[0050] Step 5 - Post-Filtering - Now, receiver R_i stores value x'_i in its memory, and follows the next program after receiving

any new x''_i, originating in Step 4:

[0051] if $x''_i - x'_i$ is divisible by a prime divisor of number m, it does nothing;

[0052] if $x''_i = x'_i - 1$ modulo m, then R_i concludes that $x_i = 1$;

[0053] if $x''_i = x'_i + 1$ modulo m, then R_i concludes that $x_i = 0$.

[0054] Next we disclose our network protocol in the case n=r and Sender S_i intends to send messages to Receiver $R_{p(i)}$ where p(i) is a permutation. The network can easily be reconfigured as follows. Since all the Senders are connected to all the channels - Sender S_i will simply send the same messages as Sender $S_{p(i)}$ would have sent to $R_{p(i)}$. Note, that no wiring and no modular addition gates (items 1 and 4 on Figure 1) are changed.

[0055] Next we disclose the network protocol in the case when n and r are not necessarily equal, and the function p from {1,2,....,n} to {1,2,...,r} gives the addresses of the messages: Sender S_i wants to send message to Receiver $R_{p(i)}$, for i=1,2,...,n.

[0056] If p(i) is an injection (that is, no Receiver gets messages from two different Senders), then the original network protocol (and filtering) works.

[0057] Suppose now, that S_1, S_2, S_3 want to send messages to -

say - R_1. Then we play the original network protocol with the substitution $x_1+x_2+x_3$ for x_1 and 0 for x_2 and x_3. Then, $x_1+x_2+x_3$ will appear at R_1 with coefficient 1. Now, in the filtering process, only those random permutations may be used that fix the order of the image of the first three numbers, for example, for the images of $x_1x_2x_3$, the image of ,x_1, should precede the image of x_2, and this should precede the image of x_3 and , This property facilitates that R_1 can recollect the bits of the long sequences which is sent to her by S_1, S_2 and S_3, respectively. Clearly, this method can be generalized to any other function p, by fixing the order of the images of variables sent to the same Receivers.

[0058] The privacy in the messaging of the network-protocol relies on the independently generated random permutations g in each round. Let us review, what R_i can learn from the bits, addressed to others. After each round of the protocol, Receiver R_i learns its own bit, and also the number of the 1-bits with the same, not-1 coefficients in the form of x'_i, for i=1,2,...,n, but R_i will not know the identity of that bits.

[0059] Although the subject invention has been described with respect to particular embodiments, it will be readily ap-

parent to those having ordinary skill in the art to which it pertains that changes and modifications may be made thereto without departing from the spirit or scope of the subject invention as defined by the appended claims.